La cryptologie consiste en l'étude des techniques destinées à **protéger l’information** **contre une attaque malveillante**. Trois acteurs font partie d’un système cryptologique : l’**émetteur** et le **destinataire du message** mais aussi l’**adversaire**. Un système cryptographique est un ensemble de protocoles et d’algorithmes qui permettent à l’émetteur et au destinataire d’échanger des données de manière sûre. Le chiffrement est la technique dont l’objectif est de maintenir le message secret. C’est l’utilisation traditionnelle de la cryptographie qui trouve son origine très ancienne dans les applications militaires. Actuellement, le **chiffrement** n’est qu’un **service** parmi d’autres offerts par la cryptographie.

Le **protocole Diffie-Hellman** est le premier système à clé publique qui a été publié (1976). Il a permis de simplifier la **distribution des clés** sur les **réseaux ouverts** comme Internet. La clé privée est une donnée secrète nécessaire au chiffrement et déchiffrement du message. Ce système permet à deux individus de partager une clé commune secrète (par l’intermédiaire d’une clé publique) sans pour autant connaître la clé de l’autre. Le cryptologue militaire Kersckoffs a énoncé que la sécurité de la cryptographie ne devait reposer que sur le secret de la clé. Le chiffrement El Gamal constitue une variante du protocole Diffie-Hellman dans lequel l’émetteur et le récepteur s’échangent en plus d’une clé publique, un message crypté.

Dès lors, un mécanisme de signature est requis pour garantir l’authenticité des clés publiques utilisées. Les clés sont ainsi assorties d’un certificat qui permet la vérification de sa provenance, notamment pour contrer une attaque classique dite de « l’homme du milieu ».

La sécurité du système de cryptage est basée sur la difficulté du **problème du logarithme discret**. Les seuls algorithmes connus permettant de résoudre ce problème sont **inapplicables en temps raisonnable.** Plusieurs modèles d’attaques existent donc pour contourner cette difficulté. Ils exploitent la connaissance de messages clairs et cryptés.